

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)	
)	
Video Device Competition)	MB Docket No. 10-91
)	
)	
Commercial Availability of Navigation)	CS Docket No. 97-80
Devices)	
)	
Compatibility Between Cable Systems and)	PP Docket No. 00-67
Consumer Electronics Equipment)	

COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC

BEYOND BROADBAND TECHNOLOGY, LLC
William D. Bauer, CEO - CTO
Beyond Broadband Technology, LLC
1140 10th St.
Gearing, NE 69341

July 13, 2010

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY	3
DISCUSSION	7
I. Downloadable Security	7
II. A New Objective; An Old Problem	8
III. Timing	10
IV. The “Minimalist Approach” to Promoting Retail Consumer Device Innovation.....	11
V. The “Successor” to CableCARDS	14
VI. Alternatives.....	17
VII. The “AllVid” Standards.....	19
<i>Encryption and Authentication</i>	19
<i>Content Ordering and Billing</i>	20
<i>Service Discovery</i>	20
<i>Content Encoding</i>	21
<i>Intellectual Property</i>	21
<i>Evolution</i>	22
CONCLUSION.....	23

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)	
)	
Video Device Competition)	MB Docket No. 10-91
)	
)	
Commercial Availability of Navigation Devices)	CS Docket No. 97-80
)	
Compatibility Between Cable Systems and Consumer Electronics Equipment)	PP Docket No. 00-67
)	

COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC

Beyond Broadband Technology, LLC (“BBT”) hereby submits the following comments in response to the above-captioned proceedings.

INTRODUCTION AND SUMMARY

"It's much harder to marry a 50-year-old technology with a brand-new technology than many of us in the new technology area thought."

Google CEO - Eric Schmidt

The Commission’s Notice of Inquiry (“NOI”) on proposed “AllVid” devices is a testament to the accuracy of Mr. Schmidt’s lament. The subject of the NOI is extraordinarily complicated and the sheer number of questions posed therein, in and of itself, counsels for a cautious approach on the part of the Commission. BBT has participated in all of the above-captioned proceedings and the Commission is now well aware of the new technology BBT has developed and tested entailing “downloadable security.” We are confident that a significant number of the filings responsive to this NOI will go into painful detail as to why, as Mr. Schmidt says, it is so hard to “marry technologies” which is one of the prerequisites of the “AllVid” proposal. Hence, we will

focus our comments specifically on the issue of how downloadable security may constitute a core technology that can act as an efficient, flexible, and effective mechanism for achieving most of the Commission's stated goals, or at least provide a workable transition to them.

This "AllVid" NOI proceeding is the latest stage in the long running saga of the Commission's efforts to implement Section 629 of the Communications Act. That section, added in 1996, directed the FCC to adopt regulations to "assure the commercial availability, to consumers of multichannel video programming and other services offered over multichannel video programming systems, of converter boxes, interactive communications equipment, and other equipment used by consumers to access multichannel video programming and other services offered over multichannel video programming systems, from manufacturers, retailers and other vendors not affiliated with any multichannel video programming distributor."¹ This mandate was conditioned by the further requirement that the regulations adopted by the Commission not "jeopardize security of multichannel video programming and other services...or impede the legal rights of a provider of such services to prevent theft of service." Congress' goal was to give consumers an alternative to leasing proprietary, non-portable equipment from their service providers, while still allowing those service providers to ensure that only authorized customers received the service packages they offered.

The Commission's initial answer to its obligation under Section 629 was to adopt the CableCARD regime, under which it was expected that consumers would have the opportunity to purchase converters and other devices that contained a slot where a

¹ 47 U.S.C. Section 549(a)

proprietary card, obtained from their service provider, could be inserted to perform the required security function. However, the Commission and industry both quickly recognized that the CableCARD was not the optimal solution. Rather, both industry and the Commission looked forward to the development and deployment of "downloadable security" solutions that would allow a consumer to purchase a device that could be quickly and seamlessly adapted to whatever conditional access its service provider was using without the need for the physical installation (and monthly rental) of a separate piece of hardware.

Today, there is widespread agreement that the CableCARD regime has been a failure. Consumers and industry alike have demonstrated through their action (or, more precisely, inaction) that the clumsy "last century" CableCARD technology is unappealing. The good news is that downloadable security is now available – something that the current consumer base, used to the flexibility and adaptability of online computer downloads of applications and programs, almost certainly will accept. What is frustrating is that instead of embracing this long sought after development, the Commission has elected to now explore a totally new approach that would go "back to the future" by replacing the physical cable card not with a less obtrusive and much more flexible downloadable option built into consumer equipment, but with a separate, proprietary, non-portable "AllVid Adapter" device that would have to be leased by the consumer to provide the security function between the consumer's purchased television set, DVR, computer, etc. and its service provider. The essence of the proposal is to start what has been a 14 year process all over again, replacing downloadable security with downloadable navigation. Were the Commission to adopt this approach, it would, in

essence be abandoning the statutory objective of providing consumers with an opportunity to receive service without having to lease a separate device. It does not have to do so. There is an alternative that can achieve most of the Commission's stated policy objectives and goals without the need to "start over." We explore that alternative here.

BBT has, on several occasions, submitted to the Commission a "White Paper" which we attach again to these comments.² We have found this to be necessary for two reasons: first, because some parties continue to misunderstand the concept of "downloadable security," the development of which has been promoted by the Commission³ and the cable industry⁴ for years; and second, because there is a tendency to use, and re-use terminology in this field, the result being that it is difficult to discuss the issues in understandable language given that the "experts" are often using the same words to mean different things. The "AllVid" proposal in some ways has fallen victim to that same difficulty.⁵ We have found it beneficial to always clarify how we are using the terminology in order to minimize confusion.

² Attachment 1; BBT White Paper on Secure Digital Communications.

³ The Commission stated over five years ago that "...development of set top boxes and other devices utilizing downloadable security is likely to facilitate the development of a competitive navigation device market." *2005 Deferral Order*, 20 FCC Rcd at 6809. It has also expressly acknowledged that *The BBTSolution™* can be deployed by MVPDs without having to obtain a waiver of the separable security rules. Public Notice, "*Commission Reiterates That Downloadable Security Technology Satisfies the Commission's Rules on Set-Top Boxes and Notes Beyond Broadband Technology's Development of a Downloadable Security Solution*," 22 FCC Rcd 244 (2007). See also *In the Matter of Comcast Corporation's Request for Waiver of Section 76.1204(a)(1) of the Commission's Rules*, Memorandum Opinion and Order, 22 FCC Rcd 228, ¶ 34 (2007) (indicating that an operator deploying BBT's downloadable security solution would not need a waiver of the integration ban).

⁴ See, e.g. Letter from Daniel L. Brenner, Senior Vice President for Law & Regulatory Policy, NCTA, to Marlene H. Dortch, Secretary, Federal Communications Commission (Nov. 30, 2005) advising the Commission of the industry's commitment to the deployment of downloadable security devices.

⁵ The use of terms like "adapter" to replace what has commonly been referred to in the MVPD industry as a "set top box" creates unnecessary confusion. Almost all of the functions of what is now called a "set top box" with separable security would be replicated in an integrated "adapter" which would also have to include additional standardized output and control protocols, or be an add-on device in addition to the

DISCUSSION

I. Downloadable Security

The BBTSolution™ is specifically designed to comply with the Commission's mandates on "separable security." It is a hardware-based solution entailing a secure microchip that acts in precisely the same manner as a CableCARD receptacle in a set-top box, DVR, or television set. The difference is that various, competitive conditional access schemes can be downloaded to the BBTSolution™ enabled device and changed as deemed necessary. The BBT enabled devices, whether leased or purchased, do not have any resident conditional access system, thus encouraging competition in the markets for both conditional access systems and consumer electronics devices.

Rather than physically replacing coded CableCARDS, with the BBTSolution™ enabled device the MVPD or intellectual property owner (in the case of broadband IP delivery) can simply download new conditional access programs from any source adhering to open specifications. This is clearly distinct from existing proprietary systems which are restricted to "downloading" only their own updates or changes to compatible proprietary devices.⁶ The Commission, we believe, well understands the difference between the two. The introduction of the ability to download, modify or totally change the security provided by multiple conditional access systems, combined with the well-

traditional "set top box." That the navigation would be separable as opposed to the security, as the Commission acknowledges, does not change the essential requirement of a "set top box" at the consumer end of the MVPD network. Changing the name to "adapter" does not make the function of that device or add-on devices any easier or less expensive, a cost which the consumer will ultimately pay, either by lease or purchase. That device, whatever it is called, was the primary focus of Congressional efforts which led to Section 629. Under the scenario described in this NOI, that device, whatever it is called, would, or could be proprietary and not designed for retail distribution, thus changing the "device" focus of the original Congressional intent in favor of a new effort to encourage retail sale of a different panoply of devices with "separable navigation," what are here defined as "smart video devices." This may be a laudable concept. It can be aided by careful use of terminology.

⁶ See, e.g., Reply Comments of NagraVision in CS Docket No. 97-80 (June 28, 2010).

established increase in security provided by hardened hardware components provides a viable long-term base from which innovation can flourish.

When we speak of “downloadable security” and the “BBTSolution™” what we are referring to is a method of establishing a highly secure communications path between a cable operator, telco video provider, DBS purveyor or even an individual intellectual property owner with a broadband server, and a viewer/customer/subscriber’s BBT-enabled set top box, game console, computer, television set or, indeed, any device that has been so enabled. The BBTSolution™ is platform agnostic. It can work with cable’s QAM technology, broadband (Internet) IP, satellites’ QPSK, broadcaster’s VSB and any other transport protocol. It is important to understand that it does not otherwise interfere with the basic business or technical constructs of those intellectual property distributors, or the material they are distributing. It simply provides a flexible, highly secure communications path in a very efficient manner. As we will detail below, it also provides other benefits by intentionally being designed to take a “minimalist” approach to the challenge presented by the Commission in this NOI of offering alternative proposals that would accomplish “...eliminating barriers to entry in the retail market for smart video devices that are compatible with all MVPD services.”⁷

II. A New Objective; An Old Problem

The NOI raises myriad questions about achieving the Commission’s newly defined objective of promoting the retail market for what has been defined as a “smart video device” – one that can, as the Commission explains it, navigate the “universe of video content made available to a viewer.” This “universe” contains all sorts of new

⁷ NOI at ¶ 2.

video sources that were not even in existence when Congress originally crafted the legislation leading to Section 76.1204 of the Commission's rules. It includes video game systems, digital video recorders, home theater personal computers, and could additionally include access to "over-the-top" (broadband video) services like internet video that have nothing whatever to do with "multichannel video program delivery." This is not your father's "set top box" or MVPD "navigation device," and shouldn't be confused with those currently available products. This is an exploration of a new world of massively integrated technology, one the Commission is right to explore.

The difficulty, of course, is that the apparent intent in promoting this new "smart video device" is to give consumers the ability to buy (or lease) and use one "control and display" device which is accessing video (and data) material from multiple currently incompatible technical transmission sources and businesses. The premise is to define and require a standardized transmission output and local (home) command and control structure for devices that would work with all sources to accomplish that goal. Even more difficult, this effort at a major technical standards amalgamation also potentially envisions, and possibly encourages, a resultant technical disaggregation of intellectual private property that is currently sold and marketed in different ways.

Thus, the Commission is not exploring just the daunting technical task of attempting to reach consensus on a single set of complex standards spanning multiple transmission (cable, broadcast, DBS, Internet, etc.), reception (television sets, DVRs, monitors, iPads and the like) and control systems (software, computers, embedded program guide products such as TiVo, "smart" television sets, "media centers" etc.), it is exploring designs that would require mandated standards which could force dramatic

changes in the current business models of numerous affected industries. BBT respectfully suggests that this may be more than any one proceeding should or could accomplish. We believe a majority of the objectives outlined by the Commission either have already been achieved or can be accomplished using existing, proved technology such as downloadable security, without the massive undertaking that would be necessitated by the “AllVid” approach.

III. Timing

Characterizing the “AllVid” concept as a “massive undertaking” is not hyperbole. We have history as a guide. Development of the DOCSIS modem standard in the cable industry – a process that involved just one transmission technology, a single industry consortium, and no conflict with existing business norms – took eleven years. The Commission’s own efforts to establish a new standard for the broadcast industry to deliver digital broadcast signals started in 1987 with the establishment of the Advisory Committee on Advanced Television Service. That effort finally culminated nine years later, in 1996, with the adoption of the ATSC digital standard (actually, 18 different standards).

There is simply no indication that the “AllVid” proposal would not be subject to the same challenges that took years to finally overcome in those two efforts. Indeed, there is every reason to believe that the challenges posed by the “AllVid” proposal would be even more daunting, and time-consuming since the sheer scope of a proposal to marry the outputs of vastly different industries and technologies into one device that could then theoretically “pick and choose” among the component parts of what could be or was delivered presents numerous and complex questions not posed by the development of the

DOCSIS modem or the adoption of a digital television standard – including questions relating to authority and jurisdiction, intellectual property and First Amendment issues. We would urge, once again, consideration of the statement by Google CEO Eric Schmidt that we quote at the beginning of these comments: *“It’s much harder to marry a 50-year-old technology with a brand-new technology than many of us in the new technology area thought.”*

The “AllVid” concept doesn’t just propose to “marry” two technologies; it proposes to marry multiple transmission technologies, all of which have their own unique requirements, with multiple potential consumer “command and control” devices, some of which will have capabilities the Commission acknowledges it cannot now imagine! To be sure, a “standard” of some sort could be forged. But its impact and potential to both promote and impede innovation cannot be imagined either. There is a better way.

IV. The “Minimalist Approach” to Promoting Retail Consumer Device Innovation

The NOI invites “alternative proposals” and recognizes that the outlined “AllVid” concept, with all its attendant premises and standards requirements is just one potential way of possibly achieving the Commission’s stated goal. That goal is specified as “eliminating barriers to entry in the retail market for smart video devices that are compatible with all MVPD services.”⁸ A cursory look at the current consumer retail market suggests that those new “smart video devices” are already appearing on retail shelves and have achieved relative compatibility with all of the MVPD services available.

Consumers can now buy both “smart” television sets and “smart devices” such as Blu-ray players that accept inputs from a cable system, a DBS provider, an IPTV system

⁸ *Id.*

or, even non-MVPD sources such as a broadband connection. These devices are already being manufactured and there is every indication that the ability to display and respond to all of those various service inputs with devices like “learning remotes” and “IR blasters” will become an industry standard without the government having to intervene in any way. Consumers can switch between the various inputs at will and, in many cases, can transport the information delivered to those inputs around the home and record that information on portable devices to the degree allowable under various rights management schemes. There is no apparent reason for the Commission to be suggesting major technical changes and the adoption of mandated standards in an effort to homogenize the outputs of all the various MVPD providers unless it is in the service of other policy objectives.

We believe several additional objectives can be identified. In the case of video, they relate directly to the issues of disaggregation and all the attendant copyright, business, First Amendment and contractual issues the Commission itself raises in the NOI. BBT does not take a position on those issues at this time other than to say that conflating them with the technical questions associated with the creation of an environment that promotes the retail sale of “smart” devices is not necessary and would likely make the entire effort far more difficult to achieve.

A minimalist technical approach based on the use of downloadable security will allow the device market to move forward almost immediately, since proved designs for platform-agnostic downloadable security now exist and are entering the marketplace. Any changes or mandates relating to disaggregation of program delivery and ultimate control of front screens, program guides, “a la carte,” program contracts, etc., would not

be foreclosed by taking the minimalist approach since in a secure communications path setting both the security and any amount of “middleware” that would respond to those issues could constantly be upgraded and altered in any embedded base of devices to adhere to the policy decisions ultimately made and tested through legislation, regulation and the courts.

An additional policy objective articulated by the Commission has been the promotion of broadband distribution and use. This is far broader than simply the question of “AllVid,” which by its very term is video-centric. Promoting broad adoption of a secure communications path downloadable security design has implications far beyond video distribution, and could have far wider implications for the adoption and use of broadband. “Minimalist” does not imply small in terms of potential impact.

An effective downloadable security design, particularly one that does not require any “trusted authority” and can have dual application in both the transmission system and home distribution between enabled devices, can promote many more uses of broadband than just MVPD video program distribution. For example, secure distribution of personal electronic health care records, secure business applications, and power grid control are just a few examples of applications that could be affected by a broad adoption of a highly flexible downloadable security design that works in both one-way and two-way environments and significantly reduces risk by eliminating the need for a “trusted authority.” The Commission’s current rules prohibiting integrated security have already spawned that new technology. The Commission need not now try to create entirely new standards and technical approaches; all that has to happen is recognition of, and active promotion of the technology that is already here.

The downloadable security approach represented by the BBTSolution™ provides the greatest latitude and flexibility for future broadband innovation. The Commission's "AllVid" proposal would, after an extended period of time when retail sale of video devices would inevitably be slowed pending the Commission's decisions on standardization, establish less flexible sets of rules and standards on a smaller, video subset of uses that could, in the future, constitute an unintended new barrier to innovation.

V. The "Successor" to CableCARDS

There is no need here to debate the merit, or lack thereof, of the CableCARD regime. The "Fourth Notice" issued as a companion to this proceeding has already solicited information on the future of the CableCARD. The record in that proceeding establishes that CableCARDS proved to be too expensive and not sufficiently flexible to spur a retail market in non-integrated devices. What exactly what went wrong with the CableCARD regime and why likely will be debated and analyzed for years.

There can be no doubt that consumers are leery of buying new devices when technology is changing so rapidly. Consumers had barely finished replacing their old Beta and VHS tape machines with DVD players and digital video recorders when equipment manufacturers began marketing Blu-ray devices and testing "remote storage DVRs." Similarly, less than a year after the transition of broadcast television from analog to digital and from standard definition to high definition displays, video programming suppliers and consumers alike were being encouraged to check out "3D" content. Lest there be any suggestion that this same phenomenon does not exist in the IP computer world, ask anyone about how often they have had to buy a new computer to

keep up with the increased speeds, more dense programming and varying WiFi standards presented to the public on an almost annual basis. Regardless of the specific answers to particular questions about “why” the CableCARD failed, it is clear that whatever the successor to the CableCARD is, it must be as flexible as possible to allow for innovation and technical advancement without the need for replacing the core component parts. That is what downloadable security, and the associated ability to download “middleware” is all about.

As we have already noted, the BBTSolution™ downloadable security design does just one thing: it establishes a secure communications path for whatever the programming or data is that is being transmitted over whichever protocol is being used. It is platform agnostic. It will assure that a cable plant enabled with the system can deliver an MVPD program package to an authorized customer. The same is true of any other MVPD transmission technology, from DBS to IPTV. It will let that same customer use a broadband modem and seek “over the top” programming from a secure server.

As important, the BBT design is flexible enough that it can also provide secure communication within the home environment between multiple BBT-enabled devices (such as a cable “set top box” or “AllVid Adapter” and a “smart video device”). It can function in-home in the same secure manner as HDMI/DTCP or DTCP IP, with one major improvement, as explained below: there would be no need for a “trusted authority.” The security “threat target” would be significantly smaller. Those “smart video devices” could even be specialized to provide particular services, such as ultra-secure video devices to receive first-run motion pictures, or medical computers used for secure transmission of private health care records. The form factor could include already

designed and tested “USB dongles” which would make most modern computers and many video devices with USB ports potentially useable as is.

Innovation would in no way be impeded, because the entire design anticipates change. Both the security and the middleware can be changed and then downloaded to the enabled device at will. As decisions are made either in the business world or the political realm about such issues as “a la carte” programming availability from MVPDs, the BBT downloadable security enabled system can be modified almost instantaneously to respond. The entire design is predicated on increasing flexibility as well as security by reducing the ‘threat target’ of protected intellectual property, be it video, data, or whatever else is sought to be secured.

Finally, and this is critically important to all the competitors in the marketplace, there is no issue of needing to “trust” a central repository for the security of “key data” or certificates - either privately or publicly controlled. The BBT downloadable security design does not require any “trusted authority.” Conditional Access (CA) or Digital Rights Management (DRM) is not “standardized” or static, but rather is left totally within the control of the individual intellectual property owner. No nationwide “target” is created for hackers, and the CA and DRM can be modified, changed, discarded and replaced on any schedule desired. Instead of trying to create a “perfect” system that cannot be broken, we have created a system that reduces both the threat of a breach and the value to the point where it is not worth the effort.

With the “AllVid” approach, the Commission has to start from the beginning with a complex and time-consuming effort to find a consensus on a whole host of new standards which would then slowly move into the marketplace. In the best of

circumstances this would take years. The Commission's estimate of having consumer "AllVid" devices distributed by all MVPDs by the end of 2012 is simply not realistic. On the other hand, downloadable security, the minimalist approach to accomplishing the same stated objectives while including the flexibility to respond to either hoped-for or mandated new business models, is already here, tested, proved and ready for deployment.

VI. Alternatives

The Commission has outlined a series of objectives and sought in this proceeding to explore alternatives. BBT respectfully suggests that while the path taken to date to promote a robust retail market for "smart video devices" has been long and cumbersome, it has, possibly inadvertently, not only spawned new technology that can achieve the immediate objective of retail device innovation, but also created a significant opening for development of many concurrent broadband uses. What's more, the Commission does not need to take major, new steps with all the attendant delay and challenge. It can simply continue on the path it has chosen and promote the new technology that achieves its goals.

By retaining and enforcing the existing prohibition on integrated security the Commission properly focuses on the key hurdle to the ability of consumers to use devices that integrate video and other information from disparate sources and technologies. So long as the providers of information are assured that they can inexpensively protect their services, offerings, proprietary property, etc., they then have no reason to object. It is when the "new" standard or the "new" technology itself requires changes to the offerings that the legal, constitutional and business issues impede technological progress. The Commission should promote the adoption and distribution of downloadable security (as

described herein) as a way to move forward while at the same time not pre-judging those other issues. The very flexibility of the downloadable security approach allows for subsequent decisions on those other issues to be accommodated.

Of course, should the Commission still decide it wants to go forward with the establishment of “AllVid” standards, it can do so totally consistent with a decision to continue the promotion of downloadable security. As noted in the following section (wherein we offer brief answers to certain specific technical issues raised in the NOI), the BBTSolution™ approach satisfies the need for security both in the transmission stream (which may be all that is necessary if the information is received on a broadband stream directly to an enabled “smart device”) and in the “home distribution” portion of the equation, between two enabled devices, such as a cable set top box and a “smart video device.”⁹ Hence, this approach could be used as a transitional stage between the current situation and an “AllVid” future. It would meld in directly with the stated objectives of many of the “AllVid” designs proposed in this NOI.

As important, there is little question of the Commission’s authority to take this approach. MVPD providers, for instance, using any transmission standard, could be encouraged to distribute a “simulcrypt” or in some cases, if necessary, a “simulcast” stream of the programming they are offering during any necessary transition. Both proved approaches are already employed in the United States and around the world. This would immediately open up the market to retail, and as important, wholesale competition

⁹ This combined capability, for instance, allows for dual use in cases where a computer or “iPad” portable type device was used both in the home and outside, something that the “AllVid” concept of split proprietary transmission path security and a “DLNA” type approach used only in the home could not. It also enables “cloud” migration of both programming and data without the need for additional devices.

in device manufacturing. It would not necessitate the Commission establishing new standards before the transition could start, immediately allowing a market to develop.

VII. The “AllVid” Standards

In the preceding sections of these Comments, BBT has outlined what we believe is a viable alternative to the proposed “AllVid” approach that can achieve both the objectives and policy goals set out by Congress in Section 629 and the new, additional objectives articulated by the Commission in the NOI. We believe that supporting and promoting downloadable security containing the attributes found in the BBTSolution™, including the ability to operate across platforms, in a one or two-way environment, and without the need for a “trusted authority,” can be implemented without delay with existing technology and without the need for the Commission to be concerned about jurisdiction, authority, or the lengthy process of establishing new national standard interfaces.

In this section, in the interest of responding as fully as possible to the Commission’s inquiry, we briefly discuss certain specific core topic-questions included in the NOI.

Encryption and Authentication

While, as the Commission notes, DTCP-IP and the use of the DLNA standard have been considered adequate by both CableLabs and the MPAA, that is true only in a limited “in-home” environment, and comes with a major administrative difficulty. By whom, and how, is the key database administered and secured? The advantage of the BBTSolution™ downloadable security approach is two-fold. First, it is not restricted to a short-distance, in-home environment. BBT enabled devices can have a secure microchip

in them that is designed to create a secure communications path between the transmission source and the individual device as well as operate to create a secure, authenticated path between specific chip-enabled devices. This is something the DLNA standard was never designed to do. Even more significant, the BBT design does not require any “trusted authority.” It eliminates that entire, very difficult, political, technical and security issue.

Content Ordering and Billing

The issues raised by the NOI regarding content ordering and billing simply do not arise with the BBT downloadable security approach. The embedded secure micro, whether in a “set top box” (or “adapter”) provided by the MVPD or built directly into a “smart video device” is part of a system establishing a secure communications path between that particular customer and the MVPD operator or “over the top” distributor. All conditions of access to the programming would be downloadable and always within the control of the purveyor consistent with the contractual purchase and sale of the programming. The conditions would be based on whatever the customer had, in fact, purchased. The BBT approach allows, for instance, for full “a la carte” delivery of product.

Service Discovery

The issues surrounding service discovery relate primarily to what can be done with the service once it is available. Universal Plug and Play protocols including “gateway advertisement” and “service browsing” are all part of the overall question of whether a seller of aggregated program packages can or is required to allow disaggregation of that product. We believe this issue is fraught with numerous legal and business issues that should not be conflated with the technical question of how best to

empower the retail “smart video device” market. The BBT downloadable approach anticipates changing “middleware” requirements, innovations and desires. The downloadable security approach can accommodate the outcome of the debates regarding disaggregation, contractual obligations and the ultimate definition of the “product” that is sold by an MVPD, whatever they may be.

Content Encoding

The Commission has recent history to study on the standardizing of codecs. The ATSC DTV standards adopted in 1996 embodying 18 different standards took 9 years to establish. The Commission is correct that if it mandated a single “AllVid” design, it would have to include at least some number of standard formats to avoid the need for transcoding content. What those various formats should be obviously would be the subject of great debate, as the Commission itself notes in the current battles over the use of various audio-video codecs on the Internet. Once again this argues for taking a “minimalist” approach of supporting and promoting a core requirement; downloadable security, and allowing the “format wars” to be fought out in the marketplace.

Intellectual Property

The series of questions posed by the Commission on “intellectual property” could be the subject of two different inquiries all on their own: one on the issues of intellectual property embodied in the various technical standards the Commission is exploring, including the potential for mandated IP patent pools, and the other on the impact and legality of creating technical structures that would by their very nature change the rights of property holders such as programmers and in many ways deprive them of the ability to control the distribution of their own property.

We cannot begin to estimate the cost and time frame required to deal with the issues surrounding various patent holders, licensing rights, patent pools and the like without a far more detailed study of the “bill of materials” that would actually be included in the Commission’s envisioned “AllVid Adapter.” We can say that those issues have already been resolved with regard to the BBTSolution™ downloadable security alternative. The BBTSolution™ secure microchip is available today for **five dollars** including a non-restrictive license as to use. The technology entailed in the chip is already under patent, or patents have been applied for. No additional IP pools would be necessary. BBT has already committed to the Commission that the specifications to write new downloadable “conditional access” protocols will be open. Hence, once again, the very real issues the Commission has raised with regard to achieving an “AllVid Adapter” solution are essentially eliminated in the alternative approach we have outlined.

Evolution

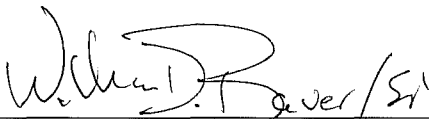
Finally, the Commission asks how it could “enable evolution in the AllVid system... in order to accommodate technological innovation over time.” This, to us, is the key question and the one that argues most strongly for a solution that is modular, starting with the “minimalist” approach we have outlined that deals with core, specific, limited issues and finds solutions that can constantly evolve. We believe that downloadable security, as embodied in the BBTSolution™ provides that answer.

CONCLUSION

The Commission has issued an incredibly comprehensive NOI asking literally hundreds of interrelated questions proposing a massive technical agglomeration and all the implications that would entail. The Commission's goals, however, may be far more easily achieved by taking a "minimalist" approach, as described in these comments. BBT respectfully requests that the Commission consider this alternative seriously. This is a case where "Occam's Razor" may, indeed, be the Commission's best guidance.

Respectfully submitted,

BEYOND BROADBAND TECHNOLOGY, LLC

/s/  /Sr

William D. Bauer, CEO - CTO
Beyond Broadband Technology, LLC
1140 10th St.
Gearing, NE 69341

Stephen R. Effros
Effros Communications
PO Box 8
Clifton, VA 20124
steve@bbtsolution.com
202-596-1305

July 13, 2010

ATTACHMENT

ONE

A “WHITE PAPER” ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION

Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system (OSDS™) which does not require the use of a "trusted authority". The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This “White Paper” is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about “information security,” it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is “downloadable,” security conditions can be changed repeatedly, depending on the use. In other words it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB “dongle”) for instance, could securely access multiple video programmers via the Internet, each with it's own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

THE BASICS

The BBTSolution has two parts; a secure microchip in the receiving device, and an “HSM” (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information on the Internet, for instance. HSM's could also be integrated into

devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. The cost of the HSM enabled equipment will vary depending on the use. The current design for cable television systems, including the computer, costs less than \$10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that the basic Hardware Security Module enabled for use on computer servers can cost half that, or even less.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a “thumb drive” or “dongle”) that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Micro, are inexpensive (they are currently priced at \$5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known “Dolby™” system is included in most consumer audio devices today.

BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBT*Solution* is that the receiving device, such as a television set, need not be a “two-way” device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBT*Solution* device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for “separable security” for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner, and descrambler) that had “integrated security”. That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or “conditional access” systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the “conditional access” components of the system. Unfortunately, CableCARDS are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers

today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, “backward compatible” with CableCARDS. One of the original objectives of BBT was to design a new “separable security” system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman's language used to describe these systems, which was subsequently adopted by the FCC, was “downloadable conditional access systems” or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption /decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A “TRUSTED AUTHORITY”

The traditional approach to establishing a secure communications path is to use a “public/private encryption key” dialog between devices. However this standard approach also requires that the “private key” be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a “trusted authority” holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a “trusted authority,” thus eliminating the two most significant drawbacks of the traditional approach.

With the BBTSolution, the “public/private” keys that enable devices to securely communicate are replaced by a “symmetrical key” approach. Keys are determined internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a “trusted authority” and the risk factor of “hacked” or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the “threat target” for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term “conditional access,” the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include “conditional access” protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus the BBTSolution has been designed in an “open” format where specifications will be made available so that anyone can design “conditional access” software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as robust as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB “stick”, which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized “conditional access”

protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be authorized only with thumb print verification as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a “virtual machine” or “tool box” that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12th power combination of encryption/decryption processes. However one can never assume that something simply can never be “broken,” so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a “software-only (DRM--”digital rights management”) approach to encryption or conditional access is subject to constant challenge. As the saying goes, “..there's a new crop of 18-year-old hackers every year!” The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional “DRM” chosen by the information provider, the ability to “download” protocols allows for other flexibility as well. For instance information stored in different formats may require that a “reader” be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a “trusted authority” and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet , in particular, can fundamentally change the way those platforms are used today.

ADDENDUM ATTACHED

ADDENDUM – I

Recent events have highlighted, once again, the validity of the reasoning behind the BBTSolution™ approach to electronic information and communications security. The experimental “hacking” of the latest proposed algorithm for use in 3G cellular telephony and the increased focus on illegal international efforts to access proprietary data from various secure repositories of corporate information has once again demonstrated the weakness in current security thinking. Software solutions and “secure repositories” or “trusted authorities” are being challenged regularly and there is no indication that this activity will stop. Indeed, it clearly is increasing.

The BBTSolution™ answer to that challenge is a design where any attack on the system is anticipated, repairable, and totally limited. There is no “trusted authority.” The “threat target” in the BBT approach can be reduced, literally, to single communications events. Each initiation of the BBTSolution™ secure communications path utilizes a totally unique and individualized creation of ephemeral keys. Those keys would have to be broken during the communications session, since once the individual session is over those keys are no longer of any relevance. Further, since each session and associated conditional access protocol is totally controlled (as to timing, duration, content, encryption, etc.) by the communicating parties, they can change any or all parameters at will. A “hacker” would have to, while the communications session was in progress, ascertain all of those variables, including the methodology and algorithm used for deriving the unique session keys. Portions of that methodology and the algorithms used are variable as well, making any single session “hack” of very limited value.

Rather than try to create a “Fort Knox” that “can’t be broken into,” BBT has taken a totally different approach, creating a security design that is so nimble and flexible that the extreme effort it would take to compromise the secure communications path could only yield a result, if successful at all, for that single, unique communication. In addition, all system administrators create their own set of variables, encryption and additional conditional access protocols, adding to the overall security of the vast majority of uses.

A REPRESENTATIVE EXAMPLE: ELECTRONIC MEDICAL RECORDS

There are several interrelated issues in the effort to shift to electronic medical records. Not only is individual security and privacy required, but the records themselves, as in the case with the Veterans Administration, for example, may be in different locations and they may not all be uniform. The use of the BBTSolution™ downloadable security design can address all of those challenges.

In order to assure privacy and authentication, a BBTSolution™ secure microchip can be embedded in a personal “USB Dongle” (a form-factor like a “thumb drive”) which also incorporates a biometric (thumb print) reader. The veteran could then visit any facility with computers having USB inputs and authenticate his or her right to access the particular medical records by establishing a secure communications path with any repository medical computer having the requisite HSM (Hardware Security Module). The encrypted thumb print data is stored directly on the resident secure microchip. The USB device will not establish any secure communication without that initial authentication. Any additional authentication required, such as a password, an account number or whatever the institution requires with its own pre-established set of conditional access rules, which would be downloaded to the receiving computer upon initiation of the secure communications path, would assure that the encrypted records were only being transmitted to the appropriate location and that only that location had the requisite information to decrypt the files. That decryption capability would, in this example, only last as

long as the secure communications path was in place.

The process also anticipates the interim “downloading” of specialized software should the sending and receiving medical facility not have the same capabilities for reading or reviewing the records. It, too, would only be useable so long as the secure communication path was intact, or limited in any other way decided upon.

Of course any other set of variables could be applied to the medical data thus downloaded. It could be time limited and then automatically discarded, it could be decrypted or left entirely encrypted and only accessible during secure communications path sessions with the personalized USB key, or it could be authorized for use by the new medical facility as a repository for the data. All of these options and many more can be made available through the use of easily developed and downloaded computer code. The key to the secure communication of the data is the initialization of the secure communications path, and the multiple options afforded the user through downloadable capability once that path is established.

While we have cited a USB thumb-drive type form factor (currently tested and ready for mass production) in this quick exploration of how the BBTSolution™ can be used to address many of the challenges of electronic health care records security and distribution, there are other form factors that could also be employed, such as a “smart card,” or the BBT secure microchip being directly incorporated into a computer laptop. In addition, it should be noted, again, that because of the flexibility inherent in the downloadable design, the same chip (in whatever form factor) used for securing electronic medical records, for instance, could also be used to view a movie, download a book, or do anything else requiring an authenticated secure communications path to multiple devices such as computers, laptops, television sets, game consoles, etc.

The whole point behind this (patent pending) approach to broadband IP security is that it can be used for multiple purposes and each one can be secured in a different way with as much or as little additional conditional access as is deemed necessary by the parties establishing the communications path. Each communications session is unique as to use, content, authentication and any other conditions chosen based on the nature and need of the communicating parties. Because of that flexibility and versatility, the BBTSolution™ security protocol enables far more uses in a more secure manner than current designs.

07 09 10

Contact: Steve Effros
steve@bbtsolution.com
202-596-1305